An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher

Rodolphe LAMPE, Jacques PATARIN and Yannick SEURIN

December 3, 2012

Definition of the Even-Mansour Cipher

$k_0, k_1, ..., k_t \in \{0,1\}^n$
$P_1, ..., P_t$ public permutations of $\{0,1\}^n$

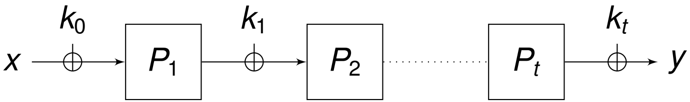

Figure: The iterated Even-Mansour cipher E.

defined in the random permutation model: the adversary has oracle access to internal permutations $P_1, \ldots, P_t$ (one can think of P_i as e.g. AES with a fixed publicly known key).

CCA-Indistinguishability

$P_1, ..., P_t, Q$ are uniformly random permutations.
E is the iterated Even-Mansour scheme with uniformly random keys $k_0, ..., k_t$.

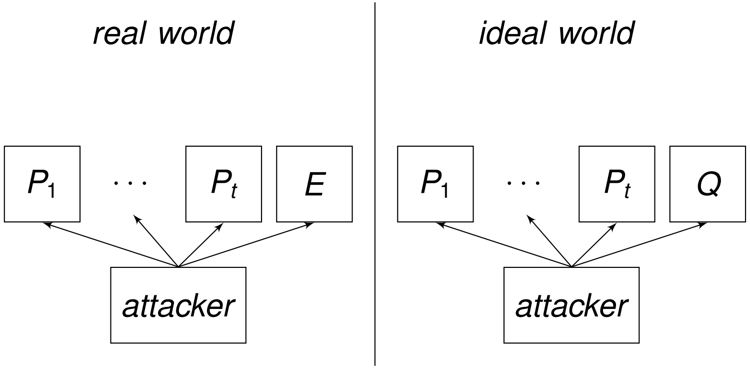

Figure: The indistinguishability game.

Previous results

"A Construction of a Cipher from a Single Pseudorandom Permutation" Even and Mansour (J.C.) :

$$\forall t \geq 1, \quad \mathbf{Adv}_E^{cca}(q) \leq \mathcal{O}\left(\frac{q^2}{N}\right) \ .$$

"Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations" of Bogdanov et al. (EUROCRYPT 2012) :

$$\forall t \geq 2, \quad \mathbf{Adv}_E^{cca}(q) \leq \mathcal{O}\left(\frac{q^3}{N^2}\right) \ .$$

"Improved Security Bounds for Key-Alternating Ciphers via Hellinger Distance" of Steinberger (eprint.iacr.org):

$$\forall t \geq 3, \quad \mathbf{Adv}_E^{cca}(q) \leq \mathcal{O}\left(\frac{q^4}{N^3}\right) \ .$$

Conjecture

Conjecture of Bogdanov et al. (EUROCRYPT 2012) :

$$\forall t \geq 1, \quad \mathbf{Adv}_E^{cca}(q) \leq \mathcal{O}\left(\frac{q^{t+1}}{N^t}\right) \ .$$

Our result

$$\forall t, \quad \mathbf{Adv}_E^{ncpa}(q) \;\leq\; \mathcal{O}\left(\frac{q^{t+1}}{N^t}\right),$$

$$\forall t \text{ even}, \quad \mathbf{Adv}_E^{cca}(q) \;\leq\; \mathcal{O}\left(\left(\frac{q^{t+2}}{N^t}\right)^{\frac{1}{4}}\right) \quad .$$

NCPA-Indistinguishability

The attacker first makes q queries to each P_j and obtains equations

$$P_j(a_j^i) = b_j^i, \forall i \le q, j \le t,$$

then he makes q non-adaptive queries to E or Q.

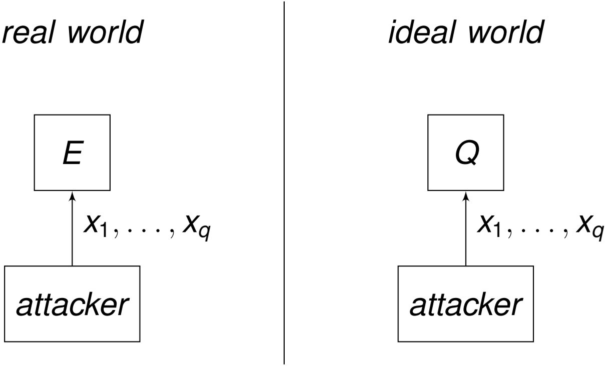

Figure: The indistinguishability game.

Statistical distance

Let μ and ν be two distributions on Ω, then the statistical distance between μ and ν is:

$$\|\mu - \nu\| = \frac{1}{2} \sum_{x \in \Omega} |\mu(x) - \nu(x)| \ .$$

Advantage

Let S_1 and S_2 be two systems, $x = (x_1, \ldots, x_q)$ be q queries and μ_x and ν_x the distributions of the outputs of S_1 and S_2 on inputs x then, the advantage to distinguish S_1 from S_2 satisfy:

$$\mathbf{Adv}_{S_1,S_2}^{ncpa}(q) = \max_x \|\mu_x - \nu_x\|$$

Application to Even-Mansour

Let $x = (x_1, \ldots, x_q)$ be any $q-$tuple of queries and
μ_0: distribution of outputs in the ideal world (Q) with inputs x.
μ_q: distribution of outputs in the real world (E) with inputs x.

We will upperbound $\|\mu_q - \mu_0\|$ independently of x to upperbound the advantage of any NCPA-distinguisher.

Dividing the problem in q smaller problems

Consider the distributions of:

Dividing the problem in q smaller problems

Consider the distributions of:

- $Q(x_1)$ with Q uniformly random, x_1 fixed.

Dividing the problem in q smaller problems

Consider the distributions of:

- $Q(x_1)$ with Q uniformly random, x_1 fixed.
- $E(u_1)$ with any E, u_1 uniformly random.

Dividing the problem in q smaller problems

Consider the distributions of:

- $Q(x_1)$ with Q uniformly random, x_1 fixed.
- $E(u_1)$ with any E, u_1 uniformly random.

Same output distribution (uniform).

Another ideal world

$P_1, ..., P_t$ are uniformly random permutations verifying $P_j(a_j^i) = b_j^i, \forall i \leq q, j \leq t$.
E is the iterated Even-Mansour scheme with uniformly random keys $k_0, ..., k_t$.
$u_1, ..., u_q$ are uniformly random.

real world	*ideal world*
inputs to E : $x_1, \ldots, x_q$	inputs to E : $u_1, \ldots, u_q$
$\boxed{E}$	$\boxed{E}$

Figure: The indistinguishability game.

Definition of world ℓ

$P_1, ..., P_t$ are uniformly random permutations verifying $P_j(a_j^i) = b_j^i, \forall i \leq q, j \leq t$.
E is the iterated Even-Mansour scheme with uniformly random keys $k_0, ..., k_t$.
$u_{\ell+1}, ..., u_q$ are uniformly random.

world ℓ	*world* $\ell + 1$
$x_1, \ldots, x_\ell, u_{\ell+1}, \ldots, u_q$	$x_1, \ldots, x_\ell, x_{\ell+1}, \ldots, u_q$
$\boxed{E}$	$\boxed{E}$
distribution μ_ℓ	distribution $\mu_{\ell+1}$

Figure: The indistinguishability game.

Advantage

μ_0: distribution of outputs in the ideal world.
μ_ℓ: distribution of outputs in the world ℓ.
μ_q: distribution of outputs in the real world.

$$\mathbf{Adv}_E^{ncpa}(q) \leq \sum_{\ell=0}^{q-1} \|\mu_{\ell+1} - \mu_\ell\|$$

Definition of a Coupling

A *coupling* of μ and ν is a distribution λ on $\Omega \times \Omega$ such that:

$$\begin{cases} \forall x \in \Omega, \sum_{y \in \Omega} \lambda(x, y) & = & \mu(x) \\ \forall y \in \Omega, \sum_{x \in \Omega} \lambda(x, y) & = & \nu(y). \end{cases}$$

Definition of a Coupling

A *coupling* of μ and ν is a distribution λ on $\Omega \times \Omega$ such that:

$$\left\{ \begin{array}{rcl} \forall x \in \Omega, \sum_{y \in \Omega} \lambda(x, y) & = & \mu(x) \\ \forall y \in \Omega, \sum_{x \in \Omega} \lambda(x, y) & = & \nu(y). \end{array} \right.$$

In other words, λ is a joint distribution whose marginal distributions are resp. μ and ν.

Definition of a Coupling

A *coupling* of μ and ν is a distribution λ on $\Omega \times \Omega$ such that:

$$\begin{cases} \forall x \in \Omega, \sum_{y \in \Omega} \lambda(x, y) & = & \mu(x) \\ \forall y \in \Omega, \sum_{x \in \Omega} \lambda(x, y) & = & \nu(y). \end{cases}$$

In other words, λ is a joint distribution whose marginal distributions are resp. μ and ν.
The fundamental result of the coupling technique is the following one:

Definition of a Coupling

A *coupling* of μ and ν is a distribution λ on $\Omega \times \Omega$ such that:

$$\begin{cases} \forall x \in \Omega, \sum_{y \in \Omega} \lambda(x, y) & = & \mu(x) \\ \forall y \in \Omega, \sum_{x \in \Omega} \lambda(x, y) & = & \nu(y). \end{cases}$$

In other words, λ is a joint distribution whose marginal distributions are resp. μ and ν.
The fundamental result of the coupling technique is the following one:
If $(X, Y) \sim \lambda$ then

$$\|\mu - \nu\| \leq \Pr[X \neq Y].$$

Example of coupling

$p = 0.5$ $\qquad$ $p = 0.6$

Example of coupling

$p = 0.5$ $p = 0.6$

Prove that, over 100 run, the second coin make more tails.

Example of coupling

$p = 0.5$ $\qquad$ $p = 0.6$

Prove that, over 100 run, the second coin make more tails.
Boring solution: Compute the binomial law.

Example of coupling

$p = 0.5$ $\qquad$ $p = 0.6$

Prove that, over 100 run, the second coin make more tails.
Boring solution: Compute the binomial law.
Elegant solution: Couple the coin's distributions !!

Example of coupling

Correlate the coin's distribution:

Example of coupling

Correlate the coin's distribution:

- If the first coin makes a tail, the second coin makes a tail.

Example of coupling

Correlate the coin's distribution:

- If the first coin makes a tail, the second coin makes a tail.
- If the first coin makes a head, the second coin makes a tail with probability 0.2.

Example of coupling

Correlate the coin's distribution:

- If the first coin makes a tail, the second coin makes a tail.
- If the first coin makes a head, the second coin makes a tail with probability 0.2.

It's clear that marginal distributions are respected and that the second coin makes more tails.

Coupling μ_ℓ and $\mu_{\ell+1}$

Using the Coupling lemma, if λ is a coupling of μ_ℓ and $\mu_{\ell+1}$ and $(X, Y) \sim \lambda$, then:

Coupling μ_ℓ and $\mu_{\ell+1}$

Using the Coupling lemma, if λ is a coupling of μ_ℓ and $\mu_{\ell+1}$ and $(X, Y) \sim \lambda$, then:

$$\|\mu_{\ell+1} - \mu_\ell\| \leq \Pr[X \neq Y].$$

Coupling for one round

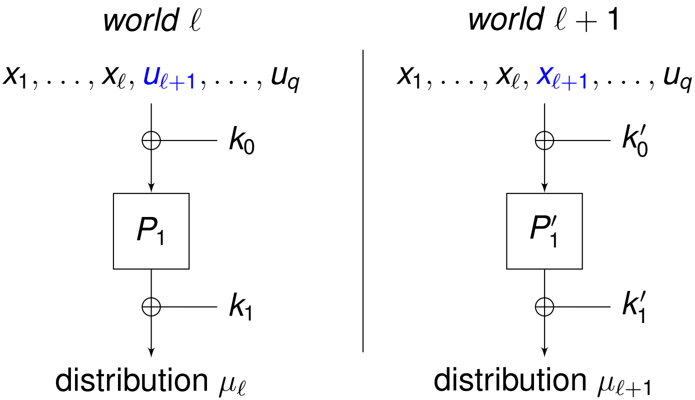

Figure: The indistinguishability game.

Coupling for one round

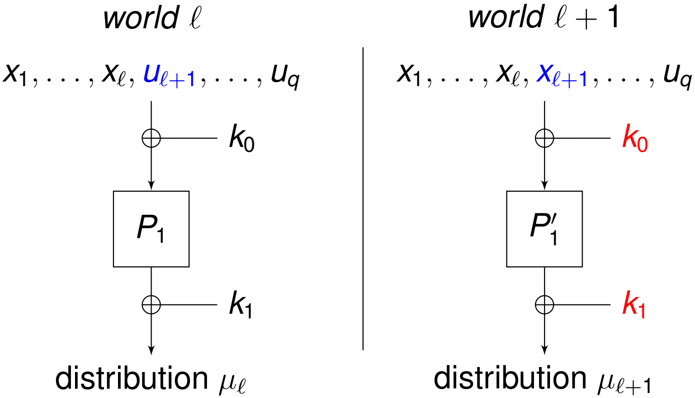

Figure: The indistinguishability game.

Coupling of the first ℓ inputs

Coupling of the first ℓ inputs

$$P_1'(x_i \oplus k_0) := P_1(x_i \oplus k_0)$$

Coupling of the first ℓ inputs

$$P_1'(x_i \oplus k_0) := P_1(x_i \oplus k_0)$$

implies a successful coupling for the *i*-th query.

Coupling of the $\ell + 1$-th query

We want:

Coupling of the $\ell + 1$-th query

We want:

$$P_1'(u_{\ell+1} \oplus k_0) := P_1(x_{\ell+1} \oplus k_0).$$

Coupling of the $\ell + 1$-th query

We want:

$$P'_1(u_{\ell+1} \oplus k_0) := P_1(x_{\ell+1} \oplus k_0).$$

If both $P'_1(u_{\ell+1} \oplus k_0)$ and $P_1(x_{\ell+1} \oplus k_0)$ are not already defined by an equation $P_1(a_1^i) = b_1^i$ or $P'_1(a_1^i) = b_1^i$ then we set the equation, the coupling is successful.

Coupling of the $\ell + 1$-th query

We can't couple if:

- $\exists i \leq q, x_{\ell+1} \oplus k_0 = a_1^i$ or
- $\exists i \leq q, u_{\ell+1} \oplus k_0 = a_1^i$.

Coupling of the $\ell + 1$-th query

We can't couple if:

- $\exists i \leq q, x_{\ell+1} \oplus k_0 = a_1^i$ or
- $\exists i \leq q, u_{\ell+1} \oplus k_0 = a_1^i$.

The probability of not coupling is upperbounded by:

$$\frac{2q}{N}.$$

Result for one round

We have

$$\mathbf{Adv}_{E_1}^{ncpa}(q) \leq \sum_{\ell=0}^{q-1} \frac{2q}{N} = \frac{2q^2}{N}$$

Result for t rounds

We use the same strategy, taking the same keys in both systems and fixing $P'_j = P_j$ when computing the outputs of $x_1, \ldots, x_\ell$.

Result for t rounds

We use the same strategy, taking the same keys in both systems and fixing $P'_j = P_j$ when computing the outputs of $x_1, \ldots, x_\ell$.

For the $\ell + 1$-th query, we can't couple if there are collisions at every round. The probability of not coupling is upperbounded by:

$$\frac{(2q)^t}{N^t},$$

because all keys are independent.

Result for t rounds

$$\mathbf{Adv}_E^{ncpa}(q) \leq \frac{q \times (2q)^t}{N^t}$$

Two weak make one strong

Composing two NCPA-secure ciphers gives a CCA-secure cipher.

Using

$$EM_{2t} \equiv EM_t \circ EM_t^{-1}$$

we find that for $2t$ rounds, one has:

$$\mathbf{Adv}_E^{cca}(q) \leq 2\sqrt{\frac{q \times (2q)^t}{N^t}} = \mathcal{O}\left(\frac{q^{\frac{t+1}{2}}}{N^{\frac{t}{2}}}\right) = \mathcal{O}\left(\frac{q^{\frac{2t+2}{4}}}{N^{\frac{2t}{4}}}\right).$$

CCA security for small number of rounds

rounds	Conjectured	Best known bound	Reference
1	$1/2$	$1/2$	(Even & Mansour)
2	$2/3$	$2/3$	(Bogdanov et al.)
3	$3/4$	$3/4$	(Steinberger)
$\dots$	$\dots$	$\dots$	$\dots$
t	$t/(t+1)$	$3/4$	(St., this paper)
$\dots$	$\dots$	$\dots$	$\dots$
8	$8/9$	$4/5$	(this paper)
10	$10/11$	$5/6$	(this paper)
$\dots$	$\dots$	$\dots$	$\dots$
$2t$	$(2t)/(2t+1)$	$2t/(2t+2)$	(this paper)

CCA security for small number of rounds

rounds	Conjectured	Best known bound	Reference
1	$1/2$	$1/2$	(Even & Mansour)
2	$2/3$	$2/3$	(Bogdanov et al.)
3	$3/4$	$3/4$	(Steinberger)
...	...	...	...
t	$t/(t+1)$	$3/4$	(St., this paper)
...	...	...	...
8	$8/9$	$4/5$	(this paper)
10	$10/11$	$5/6$	(this paper)
...	...	...	...
$2t$	$(2t)/(2t+1)$	$2t/(2t+2)$	(this paper)

Open problem: Prove the bound $N^{t/(t+1)}$ for adaptive adversaries (understand what adaptivity really brings to the adversary).


Thank You!


Thank You!